Microsoft Exchange Server

Design Considerations for Windows 2000 Active Directory with Exchange 2000 Server in Mind

Table of Contents

Table of Contents....0

Introduction....2

Points of Integration....3
- Directory....3
- Global Catalog....10
- IIS....11
- Active Directory Sites....13

Active Directory Design Issues....14
- DNS and Namespace....14
- Domains....14
- Trees....15
- Forests....16
- Domain mode....18
- Planning Domain Controllers....19
- Planning the Global Catalog....20
- Client Access to Active Directory....21
- Schema....23
- Groups....24
- Security....28
- Administration....30

Active Directory Connector....34
- Active Directory Initialization....34
- Exchange Account Management....34

Summary..... 35

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

 2000 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, Windows, Windows NT, are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Design Considerations for Windows 2000 Active Directory with Exchange 2000 in Mind

White Paper

For the latest information, please see http://www.microsoft.com/exchange

Introduction

Enhancements in technology continue to drive the functionality of information technology systems to the point that they are often an inextricable component of business. The complexities of these systems often prevent clear distinctions between the components themselves. Conventionally, components of an information technology system can be broken down into three functional areas:

- **Infrastructure services**. Core network and network operating system services that enable additional systems to be integrated. Microsoft® Windows® 2000 and Active Directory fall into this category. Microsoft Exchange 2000 Server also extends Windows 2000 and Active Directory in such a way that it also contributes to infrastructure services.
- **Application services**. These are the primary business applications organizations deploy to fulfill business requirements or to improve user efficiency and communications. Exchange 2000 Server falls into this category.
- **Internet services**. Internet services are an extension of application services that provide three-tiered applications, using Web-based technologies. These include conventional Internet services in addition to advanced Web technologies such as XML, IFS and HTTP-DAV. Windows 2000 provides the basic infrastructure for these services, but the line becomes blurred with the introduction of Exchange 2000 Server because of the implementation of many advanced technologies.

From a design perspective, Windows 2000 provides infrastructure services that, in turn, enable application and Internet services. To this point, the design of Active Directory is largely driven by the requirement to facilitate these services. This paper focuses on those areas of Exchange 2000 Server that integrate and make use of infrastructure services, which potentially impacts certain design elements.

The design and implementation of these information technology components is often haphazard, with little regard for the effects that one system has on another. Likewise, a thorough understanding of one component often leads to undue influence being placed on the design of other components.

Exchange 2000 Server has a substantial impact on all of these areas and adds value and complexity in doing so. As such, it is critical that you understand the

issues surrounding those components that are affected. Understanding these influences will assist you in planning for the integration and interdependencies that take place.

This paper consists of two primary sections:

- “Points of Integration” describes how various components of Windows 2000 and Exchange ineract. These points of integration are areas in which Exchange 2000 Server exerts influence on Active Directory design.
- “Active Directory Design Issues” discusses specific areas related to Active Directory design that you need to consider. This section provides recommendations for adjustments that you may need to make and describes the impact that Exchange 2000 Server potentially has on Active Directory and its services.

This paper assumes that you have a clear understanding of the technologies that Active Directory and Exchange 2000 Server uses. A good deal of information is available that provides an overview of Active Directory and Exchange 2000 Server. This paper discusses introductory topics only to provide clarity on specific subjects.

Points of Integration

To determine the aspects of Active Directory design that are affected by Exchange 2000 Server, a preliminary discussion of the areas of integration must take place.

Directory

Windows 2000 subsumes the conventional Exchange directory. What remains in Exchange are those functions strictly related to providing messaging and collaboration services and the administration of those services. These services, however, use Active Directory in a variety of ways.

The integration of the Exchange directory is reflected in a shift of object class for certain objects when Active Directory is compared to the Exchange 5.5 directory. The following table summarizes these changes.

Exchange 5.x Directory Object	***Equivalent Active Directory Object***	***Comments***
Mailbox	Mailbox-enabled user	This type of user has additional property pages over a standard account and has more options on the *right-click* context menu.
Custom Recipient	Mail-enabled Contact	All mail-enabled contacts have an Simple Mail Transfer Protocol (SMTP) address, although users on legacy messaging systems such as Lotus cc:Mail and Lotus Notes are represented as Contacts in Active

		Directory.
Distribution List	Mail-enabled Group	Two types of groups exist in Active Directory; Security and Distribution. Additionally, you can set the scope of the Group to Domain Local, Global, and Universal. For more information, see later sections of this paper.
Public Folder	Public Folder	You can create these types of objects only through System Manager and not through the standard Active Directory Users and Computers snap-in.

Active Directory hosts a substantial amount of information that Exchange 2000 Server uses.

Users

User objects represent one of the three security principal types in Active Directory. User objects are contained within the Domain Naming Context and are referenced in the directory by their associated Lightweight Directory Access Protocol (LDAP) context, which is referenced by Distinguished Name.

Windows 2000 user objects can also be mail-enabled, which establishes an Exchange 2000 Server mailbox in a message store. While aliases are not generated automatically, Exchange recipient policy is used to generate users' e-mail addresses.

The user object represents a single point of administration for Windows 2000 specific account activities in addition to those attributes associated with the user as an Exchange recipient.

The storage and management of user objects such as Mailboxes is completely integrated within the Active Directory Users and Computers snap-in. When you install System Manager on the computer running Windows 2000, a set of extensions is added to the standard console. This allows for the creation of an Exchange Mailbox when you define a new user account.

Groups

Windows 2000 groups are one of the powerful management aspects of Active Directory. You can use groups to greatly reduce the points of administration within the directory, thus reducing the cost of administering the system itself. Windows 2000 uses group to reduce the number of objects that require direct administration; users are placed into groups, which are further consolidated into other groups, allowing bulk administration and reference from resources. Exchange 2000 Server uses this concept of bulk administration and permission

granting, but it also expands the use of groups by using them as distribution lists to which messages can be sent.

However flexible groups may be, there are some restrictions and cautions that you must take into account when using them. Windows 2000 introduces some new concepts in groups that make them a truly functional and powerful component of Active Directory. The following two group scopes that are applicable to Exchange 2000 Server now exist within Windows 2000:

- *Security groups* are security principals within Active Directory. They are often used to group users or computers for the purpose of reducing the points of administration and providing permissions to network resources.
- *Distribution groups* are are literally a part of the distribution list available in previous versions of Exchange.

Global Groups

Global groups can contain users and computers from only the domain in which they are hosted but can be used in any domain. Global groups can contain users, computers and Global groups from the local domain. Global groups can be members of any other type of group.

You typically use Global groups as a basis for administering user membership. You can use Global groups are often defined and used to group users with similar needs into relatively narrow classifications, such as Sales Users and so on. Because the scope of Global groups is just that, the group definition is replicated as part of the global catalog. The membership of Global groups, however, is not included in the global catalog. This is because, from a security perspective, the SID of the Global group is included in the user's access token. Later sections in this paper discuss the impact this behavior has on the Exchange environment.

Note: Global groups can be converted to Universal groups as long as the Global groups do not contain other Global groups (and the domain is in native mode). This adds some flexibility in implementation.

Domain Local Groups

Domain Local groups can contain members from any domain but can be used only in the domain in which the groups. Domain Local groups can contain users, computers, and any type of group, including other Domain Local groups. Because of the restricted scope in with Domain Local groups can be used, only the definition of Domain Local groups is replicated to the global catalog. This fact, coupled with the flexibility of being able to contain any other type of group, make Domain Local groups a favorite of Active Directory administrators who are concerned with global catalog traffic.

While these types of groups can also be mail enabled, you must be aware of how using them impacts Exchange 2000 Server before you implement them. Again, this will be discussed in a later section relating to impact on design.

Note: You can convert Domain Local to Universal groups as long as they do not contain any other Domain Local groups.

Universal Groups

Universal groups can contain members from any domain and you can use them in any domain, making Universal groups a very flexible group type in Active Directory.
Universal Groups also carry some baggage with their usage. Universal group membership must be determined at the time of logon. Because the scope of Universal groups is universal, propagation of this group type is done through the global catalog. Thus, not only does the Universal group itself replicate globally, but the membership of that group also replicates. Universal groups with a large membership generate additional replication overhead the membership of the Universal group changes.

Like all other groups, Universal Groups can be security groups or distribution groups; however, Universal groups that are security groups are available only if the domain is in native mode. Refer to the section on Universal Group Usage for a discussion and recommendations on usage.

How Exchange 2000 Server Uses Groups

Exchange 2000 Server uses Active Directory groups in two ways. Conventional usage uses security groups for granting privileges and rights for administration to certain configuration and server objects related to Exchange 2000 Server. Public folders are also objects within Active Directory, which means that you can grant permissions to public folders to security groups. This is a significant improvement over previous versions of Exchange and demonstrates how Exchange is integrated with Active Directory.

The second use of Active Directory groups in Exchange 2000 Server is as distribution lists. You can use any type of group in this manner, although some groups work better than others. When a message is sent to a group, the SMTP service must expand the membership of that group. In the case of Universal groups, Exchange can gain information about the membership from any local global catalog server. For messages sent to Domain Local groups or Global groups, Exchange must obtain membership information from a domain controller in the domain in which they were created.

This works well for instances in which the recipient groups are in the same domain as the originator; however, if messages are sent to a Domain Local group or Global group that has been created in another domain, or to a Universal group that contains Global groups located in other domains, the membership must be expanded locally or forwarded to the destination domain for expansion by a local Exchange server. The first instance requires direct IP connectivity between the Exchange server performing the expansion and a domain controller for the subject domain.

Some items to consider when selecting the type of group to implement for bulk mailing are:

- How stable the group membership is. Universal groups are not well suited for groups that have dynamic membership because of the impact that replicating membership changes has on the global catalog.
- The number of domains in Active Directory. Single domains do not require a replicated global catalog.

- Usability. Global and Domain Local group membership is not visible to users outside the local domain.

Groups in Mixed Mode Domains

The description of groups given previously is accurate, but only within a Windows 2000 domain that is in native mode. While a domain is in mixed mode, groups have the same capabilities as they do in a Windows NT 4.0 environment. In fact, the limitations imposed on groups in mixed mode is just for that reason; because Windows NT 4.0 backup domain controllers may be present in a mixed-mode domain, replicating advanced concepts such as Universal security groups is not practical, and subsequently not allowed. Specific limitations to groups in mixed mode are:

- Groups can contain user objects only.
- Universal groups can be of distribution type only.
- Global groups cannot be nested in other Global groups.

Naming Contexts

Exchange 2000 Server information contained in Active Directory is not limited only to those objects readily visible within Active Directory Users and Computers. Active Directory consists of three database partitions, which are called naming contexts. Exchange 2000 Server uses all naming contexts within Active Directory. These include the domain naming contexts, the schema naming contexts, and the configuration naming contexts.

The following sections briefly describe the three naming contexts and their relationship to Exchange 2000 Server.

Domain NC

The domain naming contexts s contains all objects for the domain. This partition defines the boundaries of the Windows 2000 domain. When considering replication, it is the domain naming context that contains the majority of data that is replicated. The scope of the domain naming context is the domain in which it is contained. Thus, the domain naming context replicates only among domain controllers of the local domain.

Exchange 2000 Server fully uses the domain naming context, which hosts all information related to mail-enabled users, groups, and contacts. This information extends to security attributes that define permissions to certain Exchange 2000 Server objects in addition to specific information about the Exchange mailboxes associated with users.

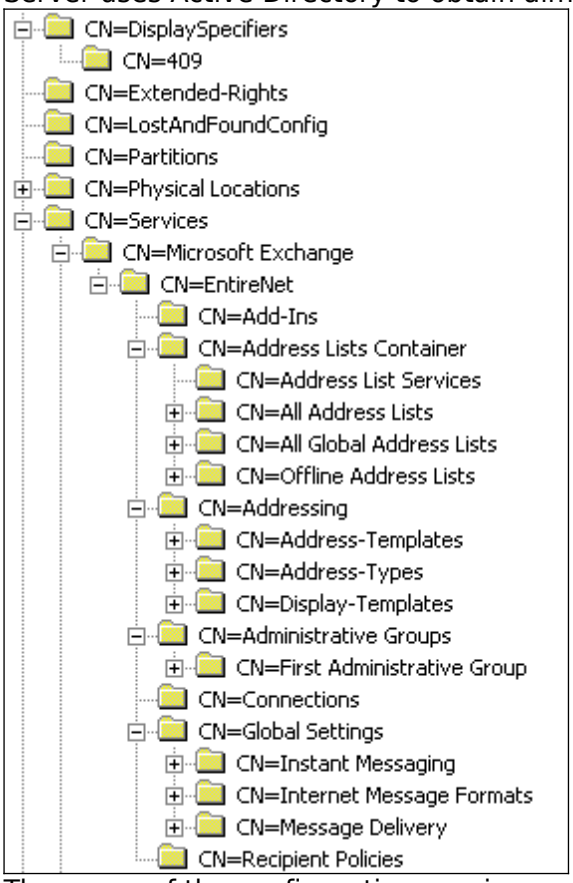
In addition to conventional information about mail-enabled users and groups, public folder definitions are also maintained within the domain naming context. Like other Active Directory objects, public folders provide an excellent mechanism for enabling single seat administration of properties, including access control. However, be aware that modification made to a security group for the purpose of access control to a public folder or bulk mailing list membership can affect other access control lists (ACLs) by which the group is referenced.

Configuration Naming Context

All message routing information, including routing and administrative groups and bridgeheads, is held within the configuration naming context of Active Directory.

To make a routing decision, the Exchange 2000 server contacts a local domain controller to retrieve this information.

A great deal of additional Exchange 2000 Server configuration information is maintained in the configuration naming context, including definitions for display specifiers, access control, and associated services. Consequently, Exchange 2000 Server uses Active Directory to obtain almost all configuration data.



The scope of the configuration naming context is global to the Windows 2000 forest. All domain controllers in the forest have a copy of the configuration naming context.

Schema Naming Context

The schema naming context provides rules that define which objects can exist within the directory in addition to attributes that are associated with those objects. The schema installed by default with Active Directory defines a large number of classes and attributes that are the foundation for all object definitions within the directory. The Active Directory schema does not, however, include initial definitions that are required for Exchange 2000 Server.

Because Exchange 2000 Server uses Active Directory for configuration and general directory information, Exchange 2000 Server extends the Active Directory schema to include a substantial number of classes and attributes specific to Exchange. For a discussion of the impact of these modifications on Active Directory, refer to the Schema section later in this paper.

Authentication

When a network client requires logon authentication, it uses its IP address and Domain Name System (DNS) settings, which are static or assigned through

Dynamic Host Configuration Protocol (DHCP), to locate an appropriate domain controller. When DNS receives the request, it attempts to match the client IP address to an Active Directory site. DNS then returns the names of the local domain controllers that can authenticate the client. The client picks a domain controller at random and notifies it to ensure that it is functioning before attempting logon. If a response is not generated within a reasonable time, the client chooses another domain controller for logon.
When a domain is in native mode, extended functionality such as Universal Security groups can be defined. As such, when each client logs on to the domain, the authenticating domain controller must pass the credentials to a local global catalog so that it can enumerate Universal Security group access. You should also allow for this additional load when determining scalability.

In summary, clients require availability of DNS, a domain controller, and a global catalog during authentication.

Exchange Server Access to Active Directory

Depending upon the type of request being made, an Exchange 2000 Server goes to different Active Directory servers to retrieve the data. Exchange 2000 Server usually establishes a number of LDAP connections to domain controllers and global catalog servers that are close by. There are two main directory activities that an Exchange 2000 server performs; address book lookups and configuration data lookups.

Address book lookups are performed whenever the Exchange server receives a request for a name to be resolved, by means of a front-end server or a back-end server. The lookup is performed to the global catalog server using LDAP over port 3268. To find a global catalog, the Exchange 2000 server queries its DNS server, which responds with a list of local global catalog servers.

When an Exchange server must read configuration data such as routing information, it connects to a domain Controller within the local domain to get this information. Once an Exchange server contacts an Active Directory domain controller for this information, the Exchange server continues to attempt to use this server in subsequent queries. This query is also performed over LDAP using port 389.

Network Transport

When you install Windows 2000, base Internet protocol stacks such as SMTP and Network News Transfer Protocol (NNTP) (if selected for installation) are configured as part of the operating system. The operating system and other components use these stacks for their own purposes; for example, it’s possible for certain directory information to replicate Active Directory information using SMTP rather than remote procedure call (RPC). The Exchange 2000 Server installation extends these stacks with additional command verbs and advanced routing components required to support specific messaging functions. These extensions are installed as a set of *sinks* registered with each protocol.

Name Resolution

Because Exchange 2000 Server is a network-oriented product, it relies heavily on the underlying network infrastructure and protocols to carry the data. Clients must communicate to servers to access collaboration data and servers must communicate with other servers to route messages. All products of this nature require a solid name resolution method. In Windows NT 4.0, the Windows Internet Name Service (WINS) provided network basic input/output system (NetBIOS) over

TCP/IP (NetBT) name resolution, and DNS for Winsock-based name resolution. In fact, all previous versions of the Microsoft Outlook® client and Exchange server have by default used the Winsock layer for communications, and so DNS was always the preferred name resolution technique. With Exchange 2000 Server, clients continue to use Winsock-based name resolution; however, all of the other Windows components such as logon and domain validation now use DNS as the primary method.

Global Catalog

The global catalog is the “white pages” of Active Directory. A single global catalog exists within the forest and consists of a partial replica of every object in each domain naming context. It is the global catalog that provides most directory services to Exchange 2000 servers and clients.

Windows 2000 and messaging clients normally query the global catalog when searching for a particular object in the directory. The global catalog is well suited for this purpose because the information within it is global, fully indexed, and cached, resulting in high-performance lookups from clients using either MAPI or LDAP over TCP port 3268.

The first domain controller in a forest is automatically installed as a global catalog server. Subsequent domain controllers, even in new domains are not labeled as global catalog servers unless you configured them as such through the Active Directory Sites and Services snap-in.

Strictly speaking, the global catalog server is a partial replica of other domain naming contexts in the forest. Global catalog servers are also domain controllers, however, so any global catalog contains a partial read-only replica of every other domain naming context in the forest, in addition to a full copy of its own domain naming context.

To understand what the global catalog server is, think of the items in the directory that are replicated to it. What goes into the global catalog is any attribute with a special property set; for example, *telephonenumber*. That property is called **IsMemberOfPartialAttributeSet**. Should this property be set to true, that attribute is replicated to the global catalog[1]. So in actuality, it is not the objects that are defined as participating in the global catalog, but attributes always contained within objects.

The global catalog is by far the most accessed component of Active Directory in terms of Exchange 2000 Server. The issues surrounding its usage can be found in the “Planning the Global Catalog” section later in this document.

Address Book Lookups

The DSProxy facilitates communication between Outlook clients and Active Directory. The two instances in which DSProxy facilitates this are:

- Proxying directory requests on behalf of clients to Active Directory (NSPI) (Outlook 97and 98)

[1] Consequently, changes made to the global catalog attribute membership trigger a complete replication of the global catalog. Plan for this when making changes.

- Referring *smart* MAPI clients directly to Active Directory (RFR) (Outlook 2000)

To achieve maximum efficiency, Exchange System Attendant resolves the name of a domain controller housing Active Directory within the same site as the Exchange server. This name resolution then goes through the DSProxy process (DSPROXY.DLL)[2].
DSProxy works with the following protocols:

- TCP/IP
- IPX
- AppleTalk

Note that DSProxy does not work over NetBIOS, including NetBIOS over TCP/IP.

IIS

Microsoft Internet Information Services (IIS) is now an integrated component of Windows 2000 and is used by Active Directory in a number of areas. The scriptable nature of Active Directory, Web-based interfaces is quite common. In fact, Web interfaces are automatically generated for printer management and printing through the Internet Engineering Task Force's (IETF's) Internet Printing Protocol and are easily created for almost any other aspect of administration.

In Exchange 2000 Server, the protocols have been removed from Information Store and now run as part of the IIS process, which has become the protocol engine. Incorporating the protocols into the IIS process allows administrators to host Exchange subsystems (protocol, storage, and directory) on different servers, making it possible to accommodate to millions of users. For example, you can design your Exchange 2000 Server topology to consist of a bank of front-end and back-end servers, which enable non-MAPI clients to connect to virtual IP-addressable front-end servers while storing messages and collaboration data on separate back-end servers.

The integration between messaging and Web services is complete. The following protocols are included with Exchange 2000 Server and use Web services provided by IIS.

Outlook Web Access

Outlook Web Access provides a browser-based interface for the basic messaging functions of Exchange 2000 Server. IIS hosts virtual roots and processing to facilitate Outlook Web Access client access to the Exchange server.

Instant Messaging

Instant Messaging allows users to see presence information for other users and provides the users with the ability to send instant communications when an immediate response is required. The user interface is designed to be lightweight and to facilitate ad-hoc communications between two users.

Instant Messaging Service runs along with Exchange 2000 Server and uses DNS and Active Directory to locate the home server for an Instant Messaging users. Instant Messaging also supports the concept of a front-end and back-end server configuration, in which the front-end servers act as a point of contact for the client. In this case however, the front-end servers are referred to as bridgeheads and redirect clients to the appropriate home server.

[2] This is signified by event 2059 for the process.

Instant Messaging is hosted through the definition of virtual servers and realms. Virtual servers group users by e-mail addresses and multiple virtual servers may exist to provide scalability. Realms effectively establish a namespace that maps an e-mail address (for example, @Microsoft.com) to a particular virtual server designated through a URL (http://im.microsoft.com). From the perspective of users, Exchange 2000 Server supports a humanized address; for example, juser@im.microsoft.com is translated into a URL such as http://im.microsoft.com/aliases/juser. Because the client uses DNS to locate the home server, you must establish a CNAME to point to the fully-qualified domain name of the home server.

Conferencing

Exchange 2000 Server Data Conferencing allows users to host virtual conferences combining data, voice, video and chat. Data Conferencing is one of the more complex features of real-time messaging that Exchange 2000 Server offers.

Data Conferencing combines several server-side components to perform conference session management and coordination. Clients can schedule online meetings and book virtual resources through Outlook 2000. The client uses the T.120 protocol that is integrated into products such as Microsoft NetMeeting. The server acts as an H.323 data conferencing server.

Exchange 2000 Server installs two Windows 2000 services to enable conferencing.

- **Microsoft Exchange Conferencing Management Service**. Conference Management Service manages the virtual resource mailboxes and conference profiles, and routes clients when they joinconferences. Conference Managers use the scope of Windows 2000 sites to direct clients to the nearest conference service.
- **Microsoft Exchange Data Conference Service**. Data Conference Service actually hosts the T.120 conference session. Data Conference Service is a standard T.120 conference bridge (MCU). Each Exchange 2000 server can host only a single MCU. For this reason, you can establish multiple MCUs to provide hosting capabilities to a large number of users.

Conferencing uses the concept of virtual conference rooms that are created on the Exchange 2000 server. Each virtual conference room is created as a standard, mail-enabled user in Active Directory.

Joining a conference is done by initially establishing a connection to the conference URL. Part of the URL specifies the dynamics of the meeting, such as the meeting ID and password (if any). These parameters are passed to IIS. If the parameters are valid, the client is redirected to the appropriate MCU and joined to the conference. At this point, IIS is no longer involved in the conference process.

SMTP

Exchange 2000 Server relies completely on Windows 2000 IIS for SMTP transport. This protocol is used for the transfer of Internet-bound messages and as the default transport for all message traffic between servers.

During installation, Exchange extends the IIS SMTP service to support some advanced features; however, these do not replace extensions that are present in IIS at the time of installation.

Enhancements include:

- Command verbs added to SMTP to enable fault-tolerant routing. Exchange 2000 Server maintains link state information, which is transferred to all servers, notifying them if a connection fails. This information is transferred between routing groups using SMTP.
- An advanced queuing engine.
- An enhanced message categorization agent.

NNTP

Like SMTP, NNTP is also a native component of Windows 2000 IIS. Exchange 2000 Server uses this service as required to provide news services as defined in Exchange Services Manager. Both SMTP and NNTP run under the Inetinfo.exe process, which is contained within Windows 2000 IIS.

Active Directory Sites

Active Directory sites are defined as one or more IP subnets with full-time, reliable connections. Unlike the sites implemented in previous versions of Exchange, an Active Directory site does not include a unit of namespace and is not a part of the Active Directory hierarchy. For example, multiple Sites can exist within a single domain. Conversely, a single site can span multiple domains. As synchronous RPC is used for replication of the domain naming context within a domain, sites can be used to define a topology that affects the links where RPC-based replication occurs. In this manner, sites help to mitigate the detrimental effect RPC communications would otherwise have if not tuned through topology. You defines sites and build *site links* to describe the network, while the Knowledge Consistency Checker automatically creates connections based on connectivity to establish an efficient, reliable replication topology.

The concept of a site has been retained from the Exchange Server 5.*x* Directory, although it is important to recognize that an Active Directory site defines zones solely in the underlying network in which high bandwidth is present. The site concept in the Exchange Directory also defined the unit of administration and namespace, and dictated message routing.

There is little integration between Active Directory sites and components of Exchange 2000 Server. Exchange uses distinct routing groups to facilitate the flow of message traffic, while Active Directory sites are used to mold the replication topology. Exchange 2000 Server uses Active Directory Sites to find a local domain controller or global catalog server for address book lookups or to access configuration information. Sites are also used by Conference Manager when redirecting clients to a conference server.

Active Directory Design Issues

If you understand how Active Directory and Exchange 2000 Server fit together, determining the impact Exchange 2000 Server has on the infrastructure services of Windows 2000 is a straightforward process. Exchange 2000 Server relies heavily on the directory and network components provided by Windows 2000, which results in two types of impact:

- **Logical**. Prerequisites exist regarding the availability and placement of certain services provided for through Active Directory. You can address these issues by making adjustments to the logical design of Active Directory.

- **Physical**. Exchange 2000 Server can have a significant impact on certain services provided by Active Directory. You must be aware of how Exchange 2000 Server uses these services to prevent system bottlenecks.

DNS and Namespace

DNS is an inextricable component of Active Directory. DNS is used for conventional name resolution and for locating services using Service Resource Records (SRV-RR). DNS is also strictly tied to the Active Directory namespace, which directly relates to the Exchange 2000 Server namespace. Exchange 2000 Server uses a couple of additional DNS services:

- **Address records**. Exchange 2000 Server uses DNS for query resolution of servers. Address record entries should exist for all Exchange servers within any given domain.
- **MX records**. Exchange 2000 Server uses Mail Exchanger (MX) records the same way as Exchange 5.5. MX records should exist to identify mail servers that service a particular domain namespace. The SMTP connector uses these records to determine preferred SMTP mail servers.
- **SRV records**. Service Resource Records (SRV-RR) are used to publish well known serivices through DNS. While Exchange 2000 Server does not register any SRV Resource Records, Exchange does use SRV Resource Records to locate domain controllers, global catalog servers, and sites.
- **Virtual namespace**. Several components of Exchange 2000 Server use IIS Web services. Services such as Outlook Web Access, Instant Messaging, and Data Conferencing all have some type of namespace associated with them. Under many circumstances, DNS aliases are established to provide users with a more friendly representation of the namespace.

Domains

The design of Windows 2000 domain topology is largely influenced by factors unrelated to Exchange 2000 Server. One interesting attribute of Exchange 2000 Server is that it works well with most Active Directory designs. A few considerations must be taken into account.

Windows 2000 domains are associated with an explicit DNS namespace. This namespace often relates to the friendly namespace users use to log on; for example, juser@redmond.microsoft.com to log on to the Redmond domain. This namespace in turn often coincides with the user's e-mail address, while other times it does not. Consider the example of juser@redmond.microsoft.com. The user's default logon name as defined by the domain and DNS namespace will probably not coincide with the intended e-mail address of the user, juser@microsoft.com.

Using User Principle Names (UPNs) alleviates the possible confusion generated by misalignment of the domain and e-mail namespace.[3] UPNs are administratively defined and assigned to specific domains or users. Normally, a single UPN exists for a forest, but several can be used. In this case, a UPN of @Microsoft.com can be created and assigned as default to all users. This provides the users with a single namespace (@Microsoft.com) that can be used for logging on and for e-mail. There are instances in which an organization may want to explicitly separate UPNs from the namespace used for e-mail. Separating UPNs from Internet e-mail addresses adds additional security by not explicitly affiliating user names with publicly known e-mail addresses.

The second issue that can impact domain design is the use of mail-enabled groups. Global and Domain Local group membership does not propagate to the global catalog. As such, these groups must be expanded on a domain controller within the hosting domain, or a lookup must occur across the wire from an Exchange server that exists in another domain. Because of this, heavily used mail-enabled groups can cause quite a bit of traffic. However, instead of adjusting your domain design, you can make these types of groups Universal instead of Global or Domain Local. You can define Active Directory groups within the following framework:

- Define which security groups are required to implement your administrative model.
- Define which of those security groups should be mail-enabled.
- Define the additional distribution lists you require and define those distribution groups.

Another consideration for group design is the membership of security groups. If you create a security group that is mail-enabled, users added to that group will also have access to the resources you grant to the group. If you add a user a mail-enabled security group with the intention of having that user receive messages sent to the group, remember that the user will also have access to the group's resources.

Trees

An Active Directory tree is defined as one or more domains arranged in a hierarchical manner, sharing a contiguous DNS namespace and two-way Kerberos trust.

Generally speaking, one tree is optimal. Multiple trees have a few minor drawbacks, such as additional namespaces to manage and query degradation from clients that do not use the global catalog; however, none of these, with the possible exception of namespaces, impact an implementation of Exchange 2000 Server.

[3] Some organizations will not want their UPNs to match their email aliases because it makes it easy for a hacker to know the logon alias for a user, simply by knowing his or her e-mail name. Therefore, some organizations intentionally avoid making the UPN the same as the user alias. This is a business decision that you make during the Active Directory design process.

Forests

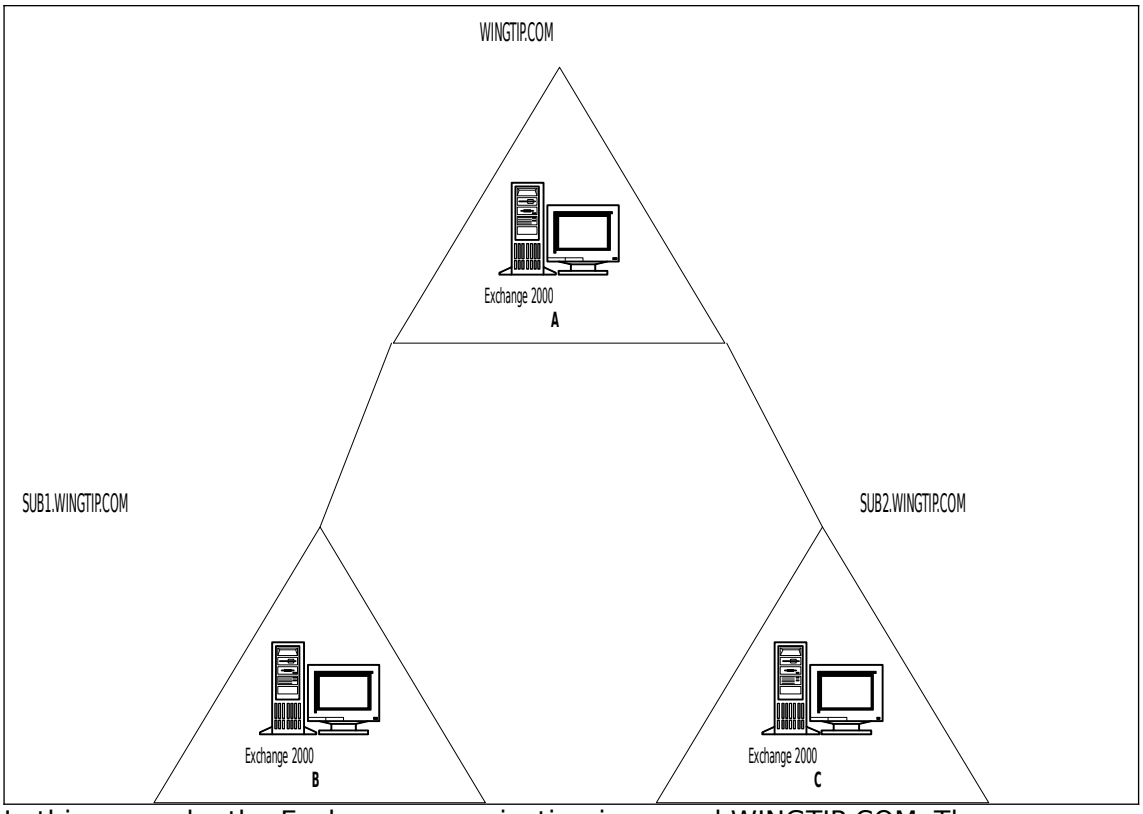
Active Directory forests consist of one or more trees that share a common configuration and schema naming context and a single global catalog. The first domain in the forest is the forest root. This domain cannot be renamed nor removed, nor can two forests be merged. All domains within a forest implicitly trust each other as a result of the transitive Kerberos trust established between domains within every tree.

Under normal circumstances, a single forest for each organization is the rule. However, there may be reasons why a company may have multiple forests after deployment:

- A company merger in which both companies have already deployed Active Directory.
- For legal reasons, which specify that directories must be completely isolated from one another
- Each department requires its own installation.
- Lack of planning and communication between departments.
- Two entities within an organization have different change control policies.

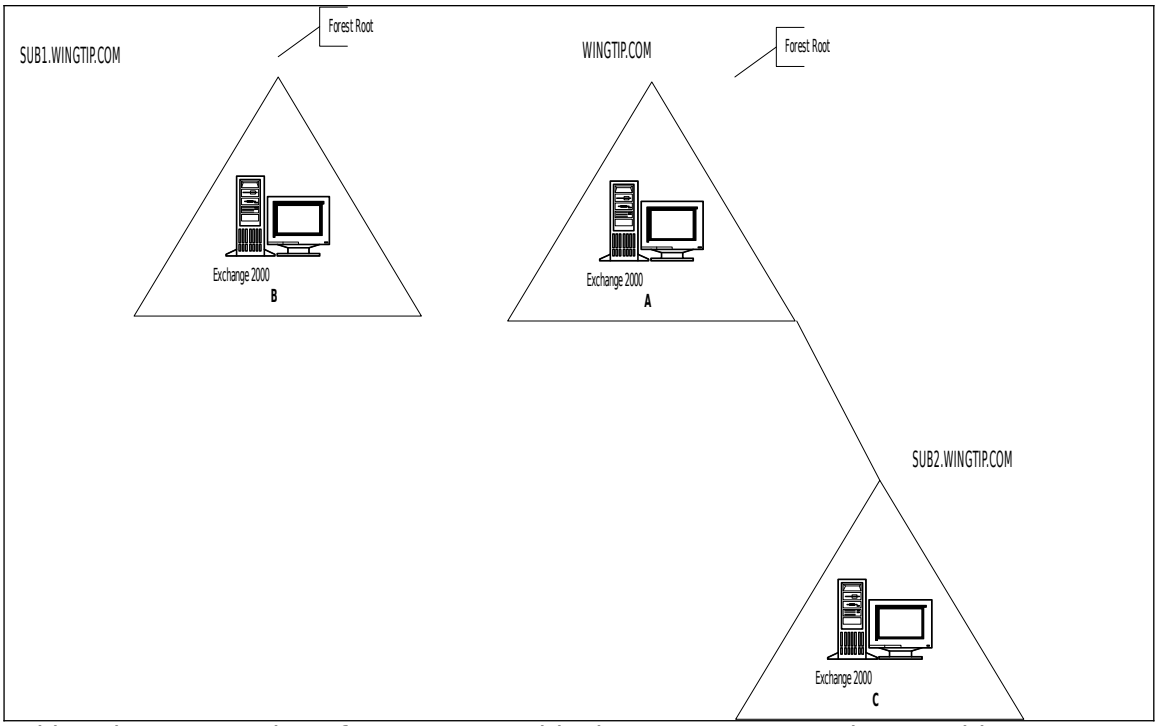
In general, infrastructures suffer as a result of having multiple forests, so you should avoid them. There are some inherent limitations to communication between forests. The most obvious is the lack of a single global catalog and non-transitive trusts. The result of this is a topology very similar to a Windows NT topology. While this is obviously not an issue with an Exchange 5.*x* system, it prohibits a homogeneous Exchange 2000 Server organization. It was possible in previous versions of Exchange for an Exchange organization to span multiple untrusted Windows NT domains. Exchange replicated across the messaging infrastructure regardless of the Windows NT topology. In Exchange 2000 Server, the Exchange organization is the Active Directory forest. As such, it is not possible for a single Exchange 2000 Server organization to span more than one forest.

Consider the example illustrated in the following diagram.



In this example, the Exchange organization is named WINGTIP.COM. The Exchange 2000 servers can exist in one or more routing and administrative groups, and all servers reference a single global catalog and store their configuration information in the same configuration naming context in the forest.

However, in the following example, let’s assume that sub1.wingtip.com was installed as a separate forest. We now have a forest named WINGTIP.COM and one named SUB1.WINGTIP.COM as shown in the following diagram. This is the most typical example of a multi-forest organization in which a department or business unit installs Windows 2000 autonomously, resulting in two forests.



Taking the perspective of namespace, this does not appear to be a problem because SUB1.WINGTIP.COM still technically falls within the contiguous namespace of WINGTIP.COM. This is where the integration ends.

First, at this point two Exchange organizations exist: WINGTIP.COM and SUB1.WINGTIP.COM. This immediately prohibits the inclusion of all Exchange 2000 servers in the same administrative or routing groups.

The second issue with two forests in this example is the global catalog and resulting address books. While it is possible to synchronize the two forests using Active Directory Connector (ADC), each forest will see the other as mail-enabled contacts.

Additional fallout from this situation relates to message routing. One of the best features of Exchange 2000 Server is found in its routing capabilities. In addition to automatic replication within a single routing group, Exchange 2000 Server also passes link state information between routing group connectors. This information allows Exchange to intelligently circumvent link failures and heal those logical links when they become available.

The last issue with multiple forests relates to calendaring information. While it is possible to assimilate the view of a single global address list and public folders, it is not possible to replicate calendar information between forests.

Domain mode

Two mode states can exist within a Windows 2000 domain. In mixed mode, the Windows 2000 domain controller appears as a Windows NT 4.0 primary domain controller to all Windows NT 4.0 backup domain controllers. While in mixed mode, the Windows 2000 domain controller replicates to down-level domain controllers as usual. All Windows 2000 domains are initially in mixed mode.

Native-mode domains dictate that no Windows NT 4.0 domain controllers are present. In native mode, there is no need to replicate information to a Windows NT 4.0 backup domain controller in a format that Windows NT 4.0 can interpret.

There is a slight difference between the two modes. In mixed mode, all information must be presented to Windows NT 4.0 in a manner it can interpret. To accomplish this, there is a group limitation in mixed mode that prevents security type Universal groups in addition to group membership and nesting functions that are not available in Windows NT 4.0

The second effect is related to SAM size and scaling. Obviously, it is not possible to replicate a SAM to Windows NT 4.0 that is larger than it can handle. This means that the same domain size limitations that apply to Windows NT 4.0 apply in mixed mode.

For these reasons, it is desirable to move to native mode as quickly as possible. Each domain in a forest can be independently moved to native mode. Keep in mind that domains in native mode still support the membership of down-level workstations and servers in addition to down-level authentication.

Planning Domain Controllers

Domain controllers in Windows 2000 hold a copy of its domain naming context and a copy of the configuration and schema naming contexts. Domain controllers also provide authentication services to both Kerberos and down-level clients.

You can promote Windows 2000 servers to the status of domain controller by using the dcpromo utility. Conversely, the same utility can be used to demote a domain controller to member server.

The number of domain controllers required for each domain and for each Windows 2000 Site is a hotly contested issue. The minimum number of domain controllers in a domain should be two, mitigating the risk of the only domain controller in the domain failing and causing the domain to “disappear”. Beyond this number, there should be at least one domain controller for each site to ensure availability to clients for authentication and applications such as Exchange 2000 Server; however, there are two additional issues that affect the number of domain controllers in any given site.

It may be that the number of locations in an organization precludes the placement of even a single domain controller in every Windows 2000 Site. In this case, the location defined as a separate site should probably be contained within another defined site directly serviced by domain controllers. If not, the site coverage algorithm will ensure that domain controllers are assigned to include themselves in defined sites that do not contain a domain controller themselves. This works the same as site coverage for global catalog servers.
These issues aside, when should an Exchange 2000 server act as a domain controller? The rule of thumb for domain controllers is that if the application that the server hosts is directory intensive or services many down-level clients, you should promote the server to domain controller status. Exchange 2000 Server often falls within that category, except when a front-end and back-end topology is used.

In a front-end and back-end topology, the front-end server handles Active Directory authentication of the client. Hence, there is an obvious advantage to

making front-end servers Windows 2000 domain controllers if they handle a large number of users.

Planning the Global Catalog

Once you understand what the global catalog is, planning the global catalog is a straightforward matter. There are only a few considerations related to the global catalog because configuration and replication are automatic.

The most obvious question is related to the number of global catalog servers required for any particular location. This is where a high level of integration with Active Directory pays off. The global catalog servers are referenced as a matter of DNS record, particularly that of the _GC SRV entries related to a particular site. In this case, there is a tight reliance on Active Directory sites, as related to the global catalog. The mechanics of this is discussed later in this paper in "Active Directory Sites."

Global catalog servers are normally a heavily used resource and the availability of the global catalog is critical. To reduce the burden on the global catalog, every Exchange 2000 server has a directory access cache called DSAccess. This allows directory lookups by Information Store and other processes such as the message transfer agent (MTA) to be cached for a period of time without the need to send the same query to the global catalog again. All directory access other than address book lookups from MAPI clients and certain portions of SMTP inbound and outbound routing go through the DSAccess process. This facility aids the performance of both the network and the Active Directory servers.

At least two global catalog servers should be available to every site. This ensures availability of the global catalog to clients and applications. Organizations with a large number of sites will probably not be able to host two global catalogs within every site. There may be times when it is not possible to hose even a single global catalog in some locations. While it is highly recommended that at least one (preferably two) global catalogs be available in every site, Active Directory compensates for occurrences where this is not the case through the site coverage algorithm. In short, Active Directory automatically affiliates domain controllers and global catalog servers with sites that do not have them present. This is done using the least cost defined in the site link topology.

Several attributes beyond those defaults are marked for replication in the global catalog. Beyond these, additional attributes may be marked for replication also, which the following table lists.

Attribute	***LDAP Attribute Name***	***Standard Active Directory***		***After Exchange 2000 Server Installation***	
		Index	**In-Global Catalog**	**Index**	**In-Global Catalog**
First Name	givenName	Yes	No	Yes	Yes
Initials	initials	No	No	No	No
Last Name	sn	Yes	No	Yes	Yes
Display Name	displayName	Yes	No	Yes	Yes
Alias	mailNickname	N/A	N/A	Yes	Yes
Mailing Address	streetAddress	No	No	No	No

Attribute	*LDAP Attribute Name*	*Standard Active Directory*		*After Exchange 2000 Server Installation*	
		Index	**In-Global Catalog**	**Index**	**In-Global Catalog**
City	l	Yes	No	Yes	Yes
State	st	No	No	No	Yes
ZIP Code	postalCode	No	No	No	No
Country	c	No	No	No	Yes
Job Title	title	No	No	No	Yes
Company	company	No	No	No	Yes
Department	department	No	No	No	No
Office	physicalDeliveryOfficeName	Yes	No	Yes	Yes
Telephone	telephoneNumber	No	No	No	Yes
Fax	facsimileTelephoneNumber	No	No	No	No
Home Telephone	homePhone	No	No	No	No
Manager	manager	No	Yes	No	Yes
SMTP Address	mail	Yes	No	Yes	Yes
Custom Attributes (all)	extensionAttribute-xx	N/A	N/A	No	No

Selecting additional attributes to be replicated in the global catalog should be well-planned. Attributes you may want to include are:

- Functional attributes that are available to mail users today. You will probably need to enable attributes included in the previous Exchange system if they are not already included.
- Additional attributes that the client must reference. Exchange 2000 Server enables most popular attributes for replication in the global catalog, but custom applications may have to reference attributes that are not.

The discovery process should include a survey of what attributes Outlook users rely on. Perhaps even more important than this is to determine whether any custom Collaboration Data Objects (CDO) or ADSI applications require certain directory data to be present. For example, a workflow application may require access to a custom attribute that holds a manager’s sign-off limit.

During installation, Exchange 2000 Server automatically tags many of the attributes that users normally require. However, there are some other important attributes, such as *department*, which are left for you to decide.

Client Access to Active Directory

MAPI Access

As excessive overhead could occur on the Exchange 2000 server because of a client request for a name; the DSProxy NSPI forwards MAPI DS requests from Outlook 97 to a global catalog server blind to the actual contents of the request. Outlook 2000 clients are referred directly to the global catalog server. For every

supported network protocol (IP, IPX and AppleTalk) and processor, a listening thread is created. Threads are dynamically added when necessary, as each thread can listen for requests from 512 concurrent client connections. Client and server connections are referenced by means of a socket mapping table that guarantees an appropriate response from Active Directory to the client initiating the request.

When DSProxy cannot contact the domain controller that was passed to it by the System Attendant (MAD), DSProxy initiates a call back to the System Attendant. The System Attendant then supplies the name of a new or different domain controller in the domain for DSProxy to use; this is called *re-targeting*.

Note that DSProxy must initiate the process of re-targeting, and this information delivery does not take place when a domain controller is taken offline or removed from a domain; in other words, a failure must happen for the re-targeting process to occur.

Traffic and Load Generated Through the DSProxy Process

When a client attempts to lookup a name, the following communications take place:

1. The MAPI client sends one network packet to the Exchange 2000 mailbox server. The packet contains the name for lookup in plain text.
2. The Exchange 2000 mailbox server *proxies* the request and sends it to a local global catalog.
3. The local global catalog returns the result to the Exchange 2000 mailbox server.
4. The Exchange 2000 mailbox server returns the result to the MAPI client.
5. The MAPI client returns an acknowledgement to the Exchange 2000 mailbox server.
6. The Exchange 2000 mailbox server proxies the acknowledgement to the local global catalog.

These six steps also represent the number of frames that a directory lookup places on the network. Even when multiple names are looked up in the directory, the name fragments are sent in the one request packet.

Outlook 2000

To be more efficient with lookups, Outlook 2000 uses a different method when accessing the address book. The Outlook client contacts the Exchange server because, by default, this is where the directory service should be and it goes through the process of contacting the DSProxy service for access. However, after the initial process of using the DSProxy service, a referral is sent to the client, informing it that future directory requests should be sent directly to the Windows 2000 domain controller that houses the global catalog.

Outlook then enters the referral in the MAPI profile:

> HKEY_CURRENT_USER \ Software \ Microsoft \ Windows NT \ CurrentVersion \

Windows Messaging Subsystem \ Profiles \ profile name \ dca740...2fe182

Value name: 001e6602
Value type: String
Value data: \\DirectoryServer.domain

(Example: \\CHOOSY.catfood.microsoft.com)

The referral mechanism reduces the load on the Exchange 2000 server and reduces the latency for address book lookups. If the Active Directory server entered in the referral fails or changes, the client would need to have the new referral written again, which would require the user to restart Outlook. In this case, the Exchange 2000 server passes Outlook a new referral to use.

A configuration that does not allow the Exchange server to pass the referral may be appropriate for certain environments. You can implement this through the following registry parameter:

HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Services \ MSExchangeSA \ Parameters

Value name: No RFR Service
Value type: DWORD
Value data: 0x1

Schema

Active Directory contains over 120 classes and 800 attributes by default. During the installation of Exchange 2000 Server, another 155 classes and 818 attributes are added to the schema. In addition, 270 attributes are marked for replication to the global catalog.

Several LDIF files containing additions to the schema are applied during the installation of the first Exchange 2000 server in the organization. It is not unusual for these modifications to take 30 minutes to complete. During this time, the Schema Master for the Active Directory forest must be available. Also, the security context performing the installation of Exchange 2000 Server must be a member of the Schema Administrators group.

The Active Directory schema is extended with new attributes, most of which start with *ms-Exch...*. Existing Active Directory attributes are also modified, which may affect what Outlook users can see.

As your organization grows, the Active Directory schema can accommodate those changes through additional extensions and modifications. should note, however, that modifications to the Active Directory schema in terms of global catalog attributes causes a complete replication of the global catalog, not just the attribute change.

For companies deploying Active Directory and installing Exchange 2000 servers at a future date, it is worthwhile to import the Exchange-specific schema changes before Active Directory becomes large. This can be accomplished by either of the following methods:

- Run Exchange 2000 Setup program with the /SchemaOnly switch
- Manually import the LDIF files on the Exchange 2000 Server installation CD

Manually importing the schema modifications defined in the LDIF files can be accomplished using the LDIFDE utility, using the syntax:

```
LDFIDE –I –f <filename>
```

Note: LDIFDE.EXE is a command line utility included with Windows 2000. For more information on LDIFDE, simply type the executable name, or see Windows 2000 Help.

Groups

The type and scope of groups you use largely depends on your particular business needs. However, different group types have a varying impact on Active Directory and Exchange 2000 Server, and you must consider these issues when mapping groups.

Universal group usage can have a rather substantial impact, because a change to the membership of a Universal group results in the entire membership being replicated to the global catalog. Even though Active Directory supports attribute-level replication, the membership for a group is held in a multi-valued attribute on the group object that is replicated in entirety. Therefore, if the group is large, a significant amount of replication traffic can be generated. To mitigate this risk, you can place user objects in Global groups and then nest these groups under a Universal group. When the membership changes for a user in the Global group, the Universal group object is not changed and thus, no replication traffic is created. The tradeoff for this configuration method is that Global groups do not have their membership directly published to the global catalog servers and this may impact the ability of an Outlook client to view the membership down to the recipient level.

The SMTP service must expand groups to which messages are destined. Membership for Domain Local groups and Global groups hosted in the local domain can be sourced through local domain controllers. Membership of Universal groups, however, can be obtained by querying the local global catalog server.
If a message is sent to a Domain Local group or Global group that has been created in another domain, or if a Universal group contains Global groups that are in other domains, there are two choices for expansion:

- Forward the message to the remote domain and let it expand there.
- Expand locally, but make direct LDAP calls to a domain controller in the remote domain to retrieve the membership. This implies that there is direct IP connectivity between the expanding server and the remote domain controller.

One disadvantage of expanding the groups locally is that the process of remote retrieval of the membership can slow down message delivery and generate more network traffic than it would take to send the message to the local domain for expansion.

Groups are also used to control access to public folders. Unlike previous versions of Exchange, Information Store does not need to expand a group (i.e. Distribution List) when a user accesses a public folder. Because all public folders ACLs are based out of Active Directory, group membership is carried in a users access token and is presented to the Exchange server on connection to the resource.

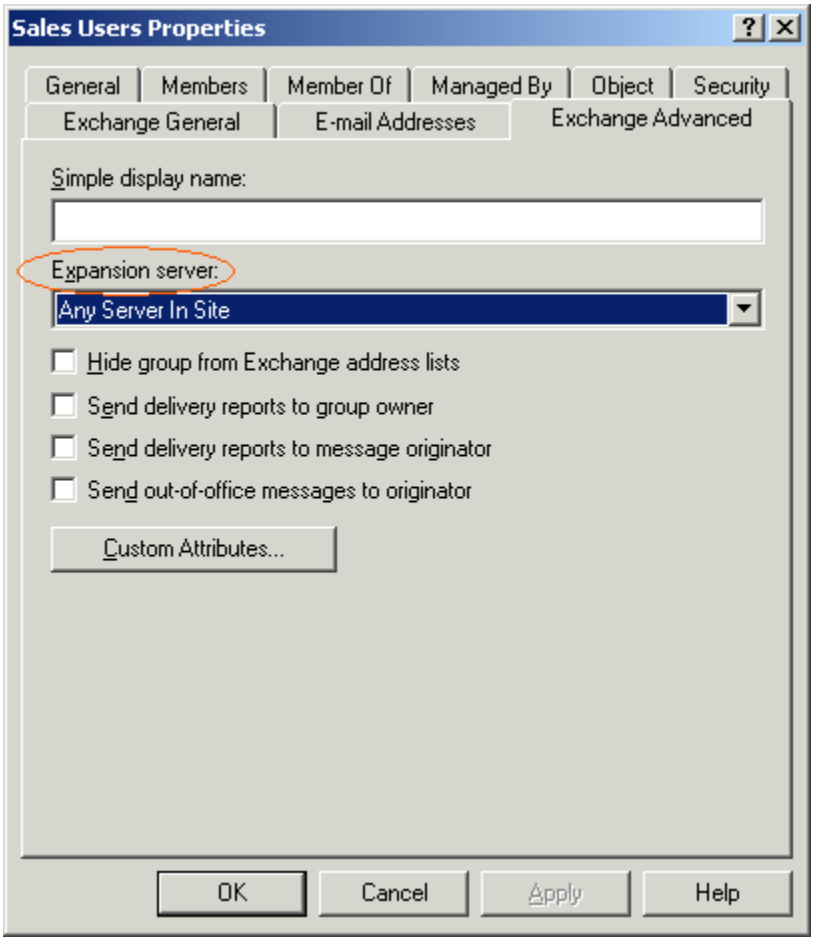
Group membership should be limited to 5,000 members, regardless of whether the groups are security groups or distribution groups. This number is not enforced but should be considered a hard limit. The design specification of Active Directory guarantees replication of up to 5,000 members but no more. In instances in which having over 5,000 members in groups is required, use nested groups to bring down the number of objects in single group membership.

The following sections will help you decide on the most appropriate way to implement your groups.

Global Group Usage

Earlier, this paper discussed the definition of Global groups and touched on their usage. The impact of Global groups within an Exchange 2000 Server environment remains an open topic.

Recall that only the Global group definition (not the membership) is replicated to the global catalog. The impact of this function from a replication standpoint is positive, because the group definition requires very little (~180 bytes) space in the global catalog. However, what happens when Exchange 2000 Server must determine the group membership based on receiving a message? The impact of this issue is determined according to the particular expansion server designated by the group itself.



The expansion server chosen dictates the point at which the Exchange server queries Active Directory to determine group membership. While often ignored in previous Exchange implementations, you should always configure this setting in a multi-domain environment.

The obvious recommendation is to choose an Exchange 2000 server that exists in the same domain as the group. Additionally, you should also consider choosing an Exchange server that also serves as an Active Directory domain controller.

Domain Local Group Usage

The primary administrative function of Domain Local groups is to consolidate the points of reference required to establish permissions to network resources. Thus, a Domain Local group normally has nested Global Groups. Domain Local groups are the reference for the ACLs of a particular resource.
The scope of this group type is the local domain. Only the definition itself is maintained in the global catalog, so as with Global groups, expansion must take place on a local domain controller.

Universal Group Usage

Universal groups are the most flexible type of group in Active Directory. When your organization is in native mode, Universal groups can be either distribution groups or security groups. If your organization is in mixed mode, Universal groups can be distribution groups only.

Use Universal groups when there is a requirement for both global membership and global usage; otherwise, you should use Global or Domain Local groups. There are two reasons for this:

- Universal groups and their membership are replicated to the global catalog. In theory, Universal group membership consists of Global groups, reducing the impact on the global catalog.
- In practice however, Universal group membership tends to be quite large, containing many user accounts. In this case, the replication impact and associated size increase substantially. The second reason concerns security. Universal groups can be nested in a global fashion. It is quite easy to inadvertently nest Universal groups to the point that they contain unintended membership.

Group Usage summary

The following tables will help you determine the attributes and usage of group types and scopes.

Security Groups

Advantages	***Disadvantages***
Can be mail-enabled by assigning an SMTP address; thus, the group can act as a Distribution List equivalent.	Accidentally placing users in the group can give unauthorized access to network resources.
Can be used for assigning permissions to public folders in Exchange 2000 Server.	User token contains group memberships. Membership in a large number of groups bloats the access token.
Useful if you want to also assign network permissions for the members in this group.	
Lowers the number of groups in Active Directory and the messaging system and time required to maintain them, because these can act as pseudo-Distribution groups.	

Distribution Groups

Advantages	***Disadvantages***
Can be used for bulk mailing.	Permissions cannot be assigned to network resources.
Can be used for Universal groups even in a mixed-mode domain.	Permissions cannot be assigned to public folders.

Domain Local Groups

Advantages	***Disadvantages***
Membership not published to the global catalog server; thus, membership changes does not cause global catalog replication.	Permissions cannot be assigned to network resources and public folders in other domains.

Outlook clients can view full user membership if they are located in the same domain in which the group exists.	Outlook users in other domains cannot view the full membership.
Membership can consist of users from any domain.	Group membership must be retrieved on-demand if expansion takes place in a remote domain.

Global Groups

Advantages	***Disadvantages***
Membership not published to the global catalog server; thus membership changes do not cause global catalog replication.	Can contain recipient objects only from the same domain.
Outlook clients can view full user membership if they are located in the same domain in which the group exists.	Outlook users in other domains cannot view the full membership.
Permissions can be assigned to network resources and public folders in any domain.	Group membership must be retrieved on-demand if expansion takes place in a remote domain.

Universal Groups

Advantages	***Disadvantages***
Membership can consist of any objects in the forest.	Membership modifications cause replication to the global catalog servers.
Outlook users in any domain can view full membership.	Universal Security groups can be created only when a domain is in native mode.
Membership never has to be retrieved from remote domain controllers.	The flexible nature of Universal groups can cause security problems associated with inadvertent nesting.
Can be used in mixed-mode domains when type is set to *Distribution.*	

There are obvious tradeoffs to implementing the various group types and scopes. Perhaps the best strategy is to use a different group type depending on the requirements for the distribution list. When planning groups, follow a logical approach that will prevent user and administrator confusion. Groups should be defined in this order:

- Define security groups to meet the requirements of your administrative model. These should include groups required for public folder access control.
- Select which of those groups should be mail enabled. Enabling all groups for bulk mailing is a bad practice.

- Define the additional distribution lists you require and define those as distribution type groups.

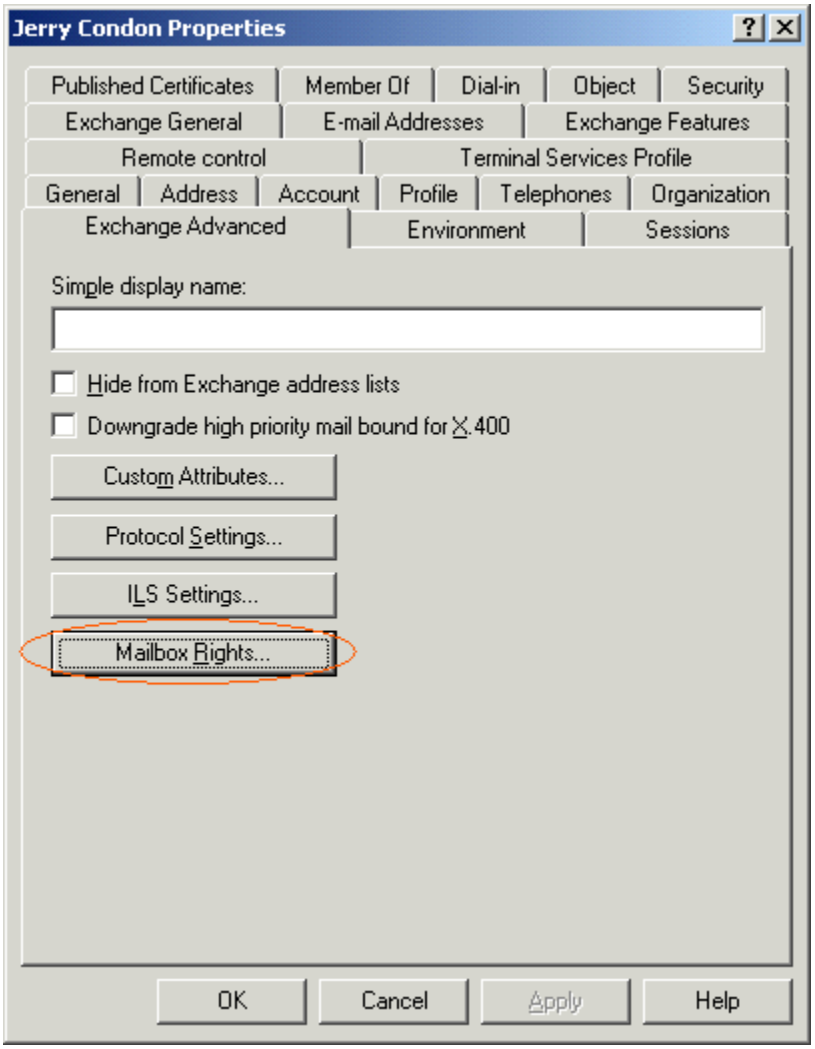
Security

Access Control

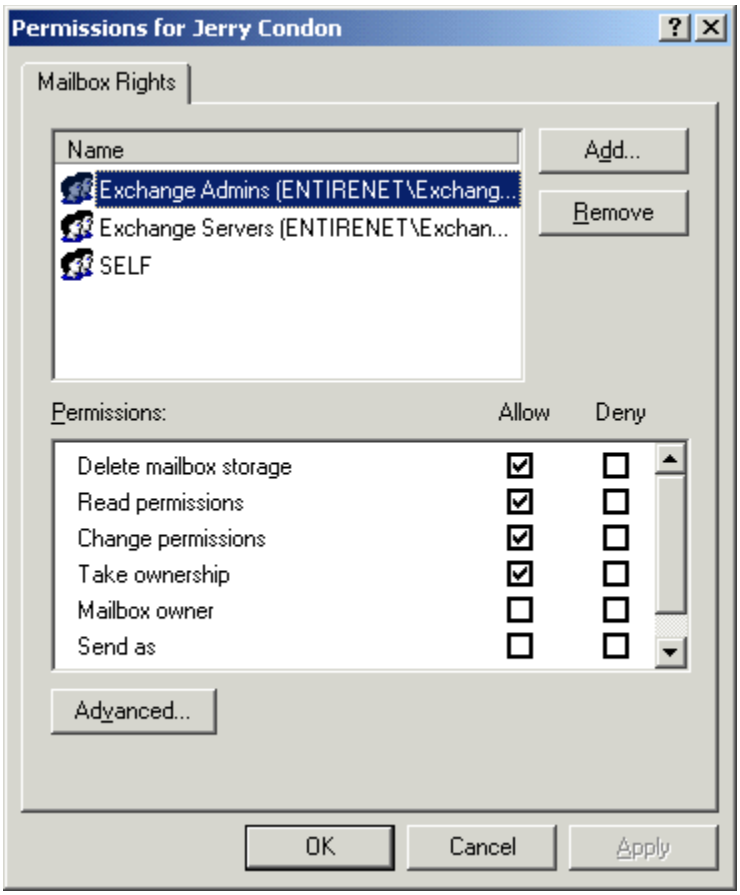
Exchange 2000 Server takes full advantage of directory and system security provided by Active Directory and underlying Windows 2000 security. The basis for all security in Windows 2000 is the Access Control List (ACL).

Access control in Windows 2000 works almost identically to access control in Windows NT 4.0. There is one major distinction, however. Access control in Windows NT was very linear and based at the object level. Active Directory supports both object- and attribute-level security, which allows a tremendous level of administrative granularity in all aspects of the system. Specifically, Active Directory influences:

- **Public folder access**. Public folder definitions become objects in Active Directory so that a variety of security attributes can be adjusted to achieve the exact level of access desired.
- **Mailbox access**. A single definition for users also applies to access rights associated with a user's mailbox.



Within every mail-enabled user is a series of property pages that dictate Exchange specific settings. These setting also apply to mailbox rights. You access mailbox rights from the advanced settings property page.



Another advantage of Windows 2000 integration is a single interface provided for security settings. In this case, Exchange-specific security properties are presented under the standard security editor dialog.

Exchange 2000 Server configuration information is also stored in Active Directory. This means that any component of Exchange 2000 Server can be efficiently delegated. This level of delegated access allows you to deploy Exchange 2000 Server to meet your business requirements without undue influence generated by the administrative model you implement.

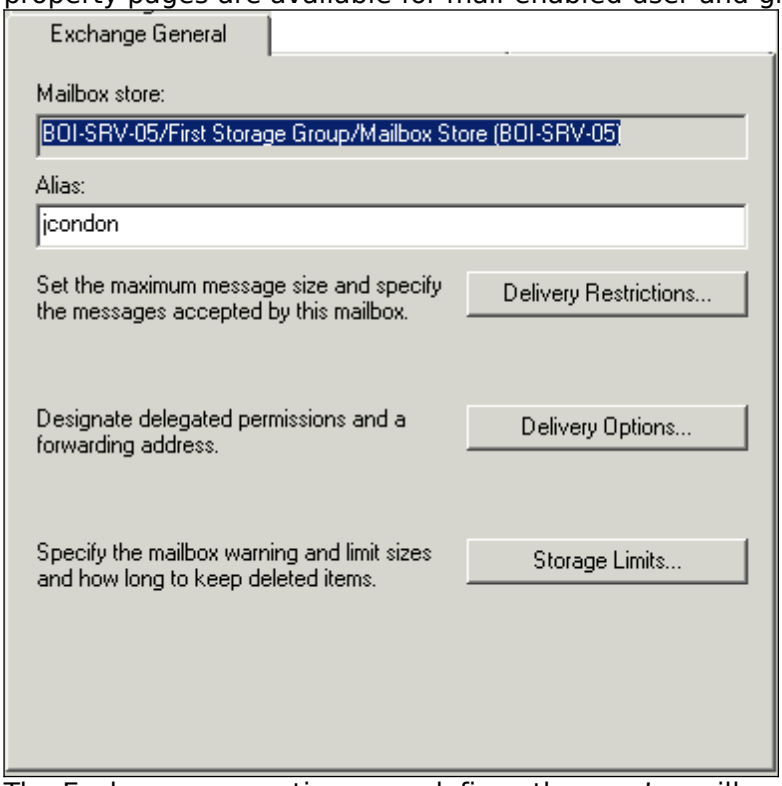
Security associated with configuration data can extend to Exchange 2000 servers, entire administrative or routing groups, or any subset of those groupings. Even certain protocols and virtual servers can be delegated. With the granularity of administration available in Windows 2000, there are simply no administrative scenarios for which you cannot account.

Administration

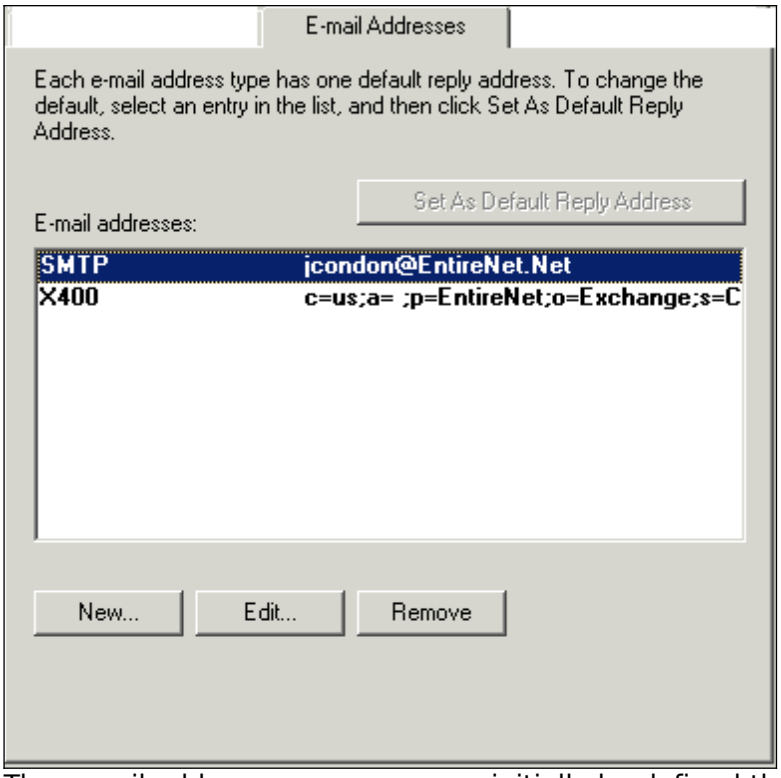
When in native mode, Exchange 2000 Server provides you with the ability to separate administrative and routing activities through the use of administration groups and routing groups. This paradigm is quite similar to the concept of using the Windows 2000 namespace for administrative purposes with little regard to the underlying network structure, which is accounted for in site topology. The membership of Exchange 2000 Server administrative groups is determined solely to fulfill administrative requirements without regard to the physical network topology or placement of servers.

There are many common points between Exchange and Active Directory that are singular in nature, and are administered as such. Other Exchange 2000 Server components, however, are specific to Exchange 2000 Server and require a separate administrative interface. Regardless of the components, all administration is performed through a single paradigm presented by the Microsoft Management Console (MMC).

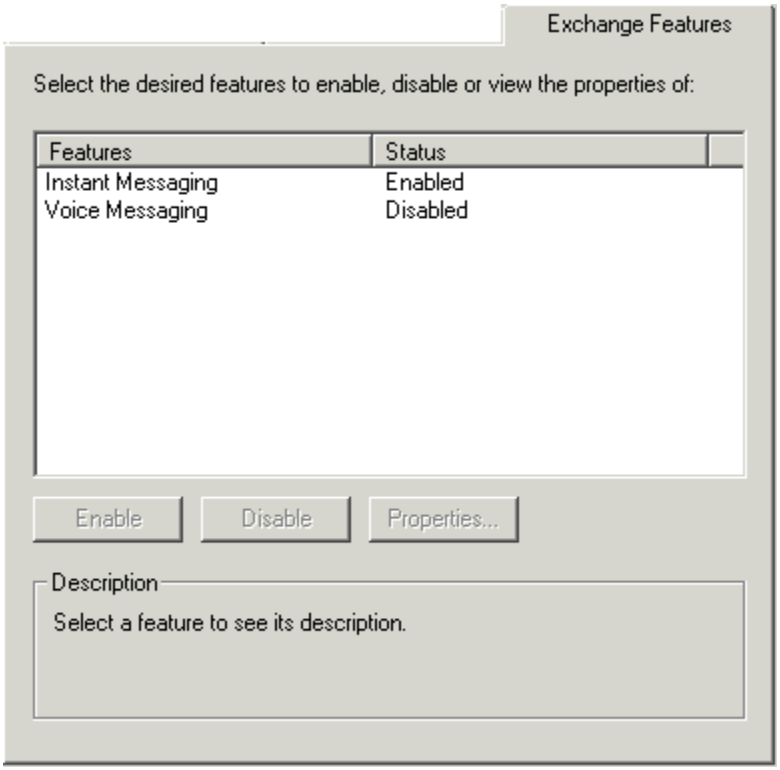
User account administration is performed entirely through the Active Directory Users and Computers snap-in. After you install Exchange 2000 Server, additional property pages are available for mail-enabled user and group objects.


Exchange General
Mailbox store:
BOI-SRV-05/First Storage Group/Mailbox Store (BOI-SRV-05)
Alias:
jcondon
Set the maximum message size and specify the messages accepted by this mailbox.
Delivery Restrictions...
Designate delegated permissions and a forwarding address.
Delivery Options...
Specify the mailbox warning and limit sizes and how long to keep deleted items.
Storage Limits...

The Exchange properties page defines the user’s mailbox alias and mailbox store properties specific to the user.


E-mail Addresses
Each e-mail address type has one default reply address. To change the default, select an entry in the list, and then click Set As Default Reply Address.
Set As Default Reply Address
E-mail addresses:
SMTP jcondon@EntireNet.Net
X400 c=us;a= ;p=EntireNet;o=Exchange;s=C
New...
Edit...
Remove

The e-mail address namespace can initially be defined through properties. This page shows the resulting e-mail addresses generated, and allows additions and modifications of e-mail addresses.

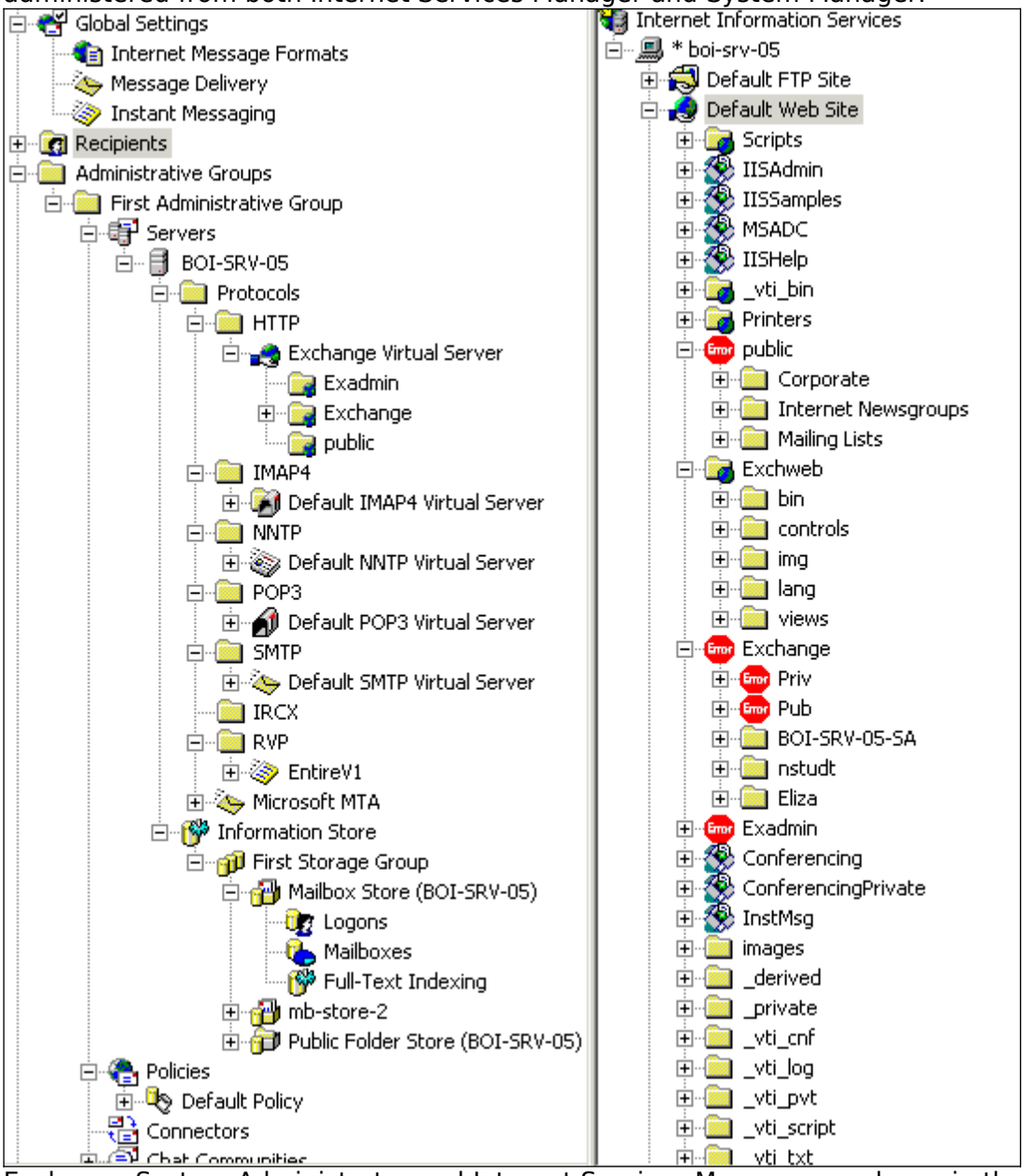


The **Exchange Features** tab initially shows user-based administrative options for Instant Messaging and Voice Messaging.

The **Advanced Feature** property page shown earlier has a number of user administrative functions such as mailbox rights, preferred ILS server and individual protocol settings.

All other administration largely takes place within System Manager. Even so, components such as public folders can be administered through both System Manager and Users and Computers Manager.

Exchange 2000 Server wholly relies on Windows 2000 network services administered through Windows 2000; however, services such as IIS are administered from both Internet Services Manager and System Manager.



Exchange System Administrator and Internet Services Manager are shown in the left and right panes respectively in the previous illustration. As you can see from the administrative interfaces, many of the virtual directories defined in IIS are also present within the Exchange System Administrator. Actually, the genesis of

these virtual directories was through Exchange itself. During the installation and configuration of Exchange 2000 Server, several virtual servers are established by Exchange. These are implemented as virtual directories within IIS.

Administration of the virtual servers and IIS virtual directories is performed through both interfaces. Ultimate control over the service state and permissions is maintained by Exchange. Some functions specific to the Web side of the services can be administered through Internet Services Manager. These functions include conventional Web administration such as URL specification, directory permissions, and document inclusion.

Active Directory Connector

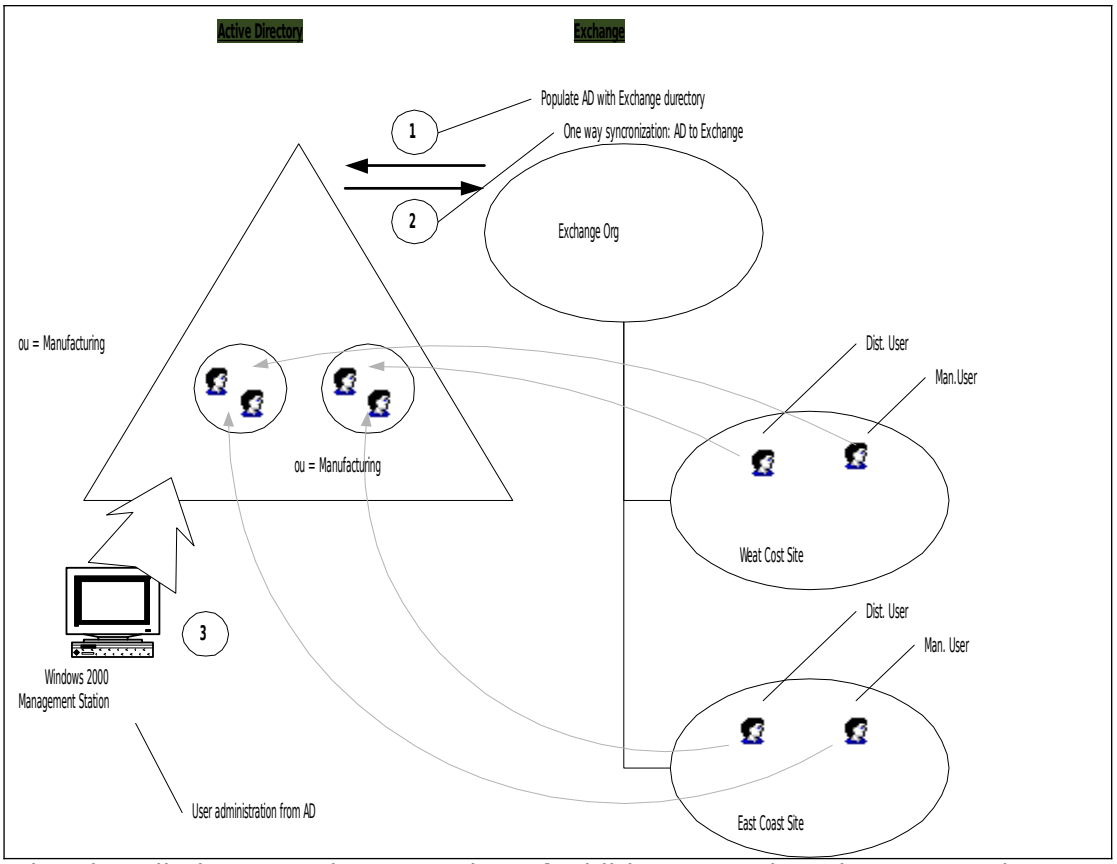
Active Directory Connector (ADC) consists of a replication and mapping engine in addition to providers for both Exchange 5.5 and Active Directory. ADC provides an excellent mechanism for replicating an Exchange 5.5 directory with that of Active Directory.
ADC works through administratively defined replication agreements, which define the direction of replication, schedule for replication, and placement of replicated objects.
There are several scenarios suited for ADC:

Active Directory Initialization

From an administrative perspective, Exchange 5.5 implementations represent a complete and timely corporate directory. One logical use of ADC is to provide an initial synchronization to populate Active Directory.
This technique is performed by establishing a one-way agreement in which Exchange mailboxes are replicated to Active Directory.

Exchange Account Management

ADC is a great tool for transitioning management from the legacy Exchange environment to Active Directory. Assuming that an initial synchronization between Exchange and Active Directory has been performed, the connection agreement is modified so that only information within Active Directory is synchronized back to Exchange. This allows complete administration of user accounts and associated mailboxes from Windows 2000.
This approach relieves collaborative administration often present in organizations. Those organizations that currently are dealing with multiple departments sharing administrative responsibility within a site will appreciate being able to separate the administrative authority within Active Directory. Once user objects are replicated to Active Directory, you can administer both Windows 2000 user accounts and Exchange mailboxes through Active Directory.



When installed, ADC makes a number of additions to Active Directory's schema to reflect the additional user attributes exposed. Additional display specifiers and administrative wizards are also installed. The impact of these changes on Active Directory is nominal.
A great deal of documentation is available on ADC. For specific information on deployment and usage, see http://www.microsoft.com/exchange/prodinfo/2000/ActiveDirectory.htm.

Summary

Windows 2000 and Active Directory introduce a number of new concepts and technologies that enhance the functionality of the network system infrastructure. Exchange 2000 Server is the first application to fully use all aspects of Active Directory. Exchange 2000 Server supports most Active Directory designs without placing excessive design restrictions on the latter.

Access control and group usage are perhaps the two areas that require the most planning. Because Active Directory groups are used both for access control and bulk mailing lists, careful planning is required to prevent inadvertent modifications to group membership that adversely impacts system security.